State of Wisconsin
Department of Administration
Division of Enterprise Technology

SECURITY

Effective Date: 8/1/17

# Maintenance Standard

## Purpose

The Maintenance standard provides documentation to plan, schedule, and provide routine and non-routine maintenance to Division of Enterprise Technology (DET)/State IT systems and system environments as required by the Maintenance Policy.

## Standard

Maintenance for DET/State IT systems and system environments must be conducted routinely to retain the effectiveness and security of the system/environment. Only approved maintenance can be performed and must follow the DET Change Management Procedure. All appropriate security measures for the DET/State IT systems and system environments must be adhered to (MA-2, MA-4).

DET must ensure that no system or software for infrastructure systems/services, as defined in the Configuration Management Database, CMDB, is allowed to fall out of vendor maintenance/support without approval via the DET Exception Procedure.

Regardless of the location where maintenance occurs, the following must be included:

### Scheduling

- Maintenance schedules must be scheduled for implementation with consideration to incur the least amount of service interruption for the end-users, while being able to coordinate with vendors and staff, as needed (MA-2). Note: DET/Agency maintenance/update freeze dates may be established to accommodate known fluctuations in staffing levels (e.g. holidays) or business needs (e.g. high processing times).

### Personnel Accountability

- Determine, document, and maintain a log of the role and specific individual(s) who are responsible for the approval of maintenance of DET/State IT systems and system environments (MA-2, MA-5).
- Designate and document internal maintenance personnel who have required authorizations and technical competence to approve and monitor the work of vendor personnel performing maintenance (MA-2, MA-5).
- Documentation of the role/individual(s) who will perform the maintenance services, along with contact information for the individual(s) must be current and available for reference (MA-2, MA-5).
- All internal and/or external maintenance personnel must have sufficient training to perform or oversee the maintenance being conducted (MA-2, MA-5).

- All internal and/or external maintenance personnel either must have the required access authorizations or be monitored by internal personnel with the required access authorizations (MA-5).
- IT Security awareness training for all internal and external IT maintenance personnel must be current prior to accessing DET/State IT systems and system environments (AT-2, AT-3, MA-5).
- Technical training for external IT maintenance personnel providing maintenance must be sufficient for competency in the appropriate DET/State IT systems and system environments prior to providing maintenance services (AT-2, AT-3, MA-5).

### Clearance for equipment

- Information system maintenance tools used by external IT maintenance personnel must be checked for improper modifications (MA-3).
- All electronic media containing diagnostics software must be scanned for malicious code (e.g. virus, malware, Trojan) before the media is utilized as part of maintenance services (MA-3).
- After maintenance is complete, all tools or software used for maintenance must be void of DET/State information and verified clean via sanitizing or destruction before it can leave DET/State IT systems and system environments (MA-2, MA-3). Exceptions for removing equipment prior to sanitation or destruction must be approved by the DET Exception Process (MA-3).

### Maintenance Tracking

All maintenance services must be documented via the DET Change Management Procedure to provide record of the following information:

1. The date and time (begin and end times) of the maintenance service (include for each day of the service) (AU-2, MA-2);
2. Technician Information
    a. Local (DET) personnel: name/division/contact information of the individual performing the maintenance(MA-5);
    b. External personnel: document the name of the employee escort for the maintenance technician along with the name/company/contact information of the individual performing the maintenance (MA-5);
3. A description of the maintenance performed; and,
4. A detailed list of equipment removed or replaced including identification, control, or serial numbers (MA-2, MA-4).

## Definitions

- Agency - State of Wisconsin legislatively defined Departments and all customers of DET services, equipment, and/or technologies.

Effective Date: 8/1/17

- DET/State information - Any information that is created, accessed, used, stored, or transmitted by an Agency and/or DET.
- DET/State information systems and system environments - All equipment or services used to input, store, process, transmit, and output information, including, but not limited to: network devices, servers, databases, printers, Internet, email, physical, virtual, cloud, and applications accessible to and/or managed by DET.
- External location(s) - Any physical facility or virtual/cloud location outside of the defined internal locations which house DET/State IT systems and system environments.
- External personnel - Individual(s) with appropriate training who do not work for directly for DET but may be contracted or otherwise approved and authorized by DET to conduct maintenance/updates/service activities, in person or virtually, on DET/State IT systems and system environments.
- Internal location(s) - Include any physical facility or virtual/cloud location owned or leased by DET which house DET/State IT systems and system environments.
- Maintenance - Maintenance, repair, updates and/or testing of DET/State IT systems and system environments.
- Maintenance supervision personnel - Individual(s) in DET with the required access, authorization, and training to supervise the maintenance/update/service/testing activities of vendor personnel, in person or virtually, on DET/State IT systems and system environments.

## Compliance References

IRS Pub. 1075
NIST 800-53 Revision 4

## Exception Process

Exceptions to this and all DET Security policies or procedures must follow the DET Exception Procedure.

## Document History/Owner

This standard was developed as required by the Department of Administration, DET Information Technology Security Policy Handbook, under the authority of Wisconsin State Statute 16.971.

This standard is effective upon approval and publication until retired. Revisions and updates continue the effective date by documenting required changes over time.

Ownership for this standard is assigned to DOA, DET Bureau of Security. As such, the DOA, DET Bureau of Security is responsible for the maintenance, update(s), and review of this document annually before the anniversary of the effective date.

Effective Date: 8/1/17

| Version | Approval/Revision/Review Date | Description | Approver/Author, Title |
|---|---|---|---|
| .1 | 5/26/2016 | Original Draft | Bill Farrar, Compliance Analyst |
| .2 | 6/16/2016 | Revisions and formatting | Tanya Choice<br>Cybersecurity Compliance Consultant |
| .3 | 7/12/16 | Revisions and formatting | Tanya Choice<br>Cybersecurity Compliance Consultant |
| 1. | 7/11/17 | Final Approval | Bill Nash<br>CISO |

Authorized and Approved by:

Bill Nash Bill Nash 7/11/17

Print/Type Signature Date

Division of Enterprise Technology-Bureau of Security

Chief Information Security Officer